

PatternEx その能力の証明

Proficio は AI 技術の広範な検証の結果、世界中で PatternEx を展開します



“PatternEx は我々の SOC
ビジネスに即座に非常に
大きな価値を与えます”

Jeremy Vance, SVP of
Technology and Security,
Proficio

Proficio とは

- 米国の MDR ランキングで 21 番
- 世界中に SOC を展開
- ワールドワイドで数百の顧客を持つ

PatternEx のベネフィット

- SOC アナリストの効率の向上
- サイバーキルチェーンのすべての段階にわたる AI モデルのカバレッジ
- クライアント固有の脅威に対するカスタム AI モデル
- キルチェーン全体および長期間にわたる脅威の自動相関機能
- 展開が簡単な 100 以上の AI モデル
- 既存の SOC ワークフロー内での統合

ビジネスおよび技術的な問題

Proficio は SOC の効率を絶えず改善しており、顧客のリスクを軽減するために複雑な脅威を見つけるための追加の方法を探していました。多数の SIEM ルールとアラートを監視するセキュリティアナリストのチームで強力なサービスを提供していましたが、AI ベースのセキュリティ分析アプローチを追加すると、脅威をより迅速かつ正確に検出できます。Proficio は、さまざまなテクノロジーベンダーとデータ管理アプローチを含む洗練されたグローバル環境を運営しています。これには、ワークフローに簡単に統合できるソリューションが必要です。

導入検討テストの結果

Proficio は、以下を含む厳しいテストを行った上で PatternEx を選択しました。

- 16 の AI モデル (5 つの異常値検出器と 11 の分類器) と、サイバーキルチェーンのいくつかのステージでサンプリングされた 100 のセキュリティ分析のテスト。
- ファイアウォール、DNS、AD を含む複数のログおよびイベントデータソースにわたるリアルタイム処理。
- クライアントデータの分離と規制コンプライアンスを検証するマルチテナンシーテスト。
- クライアント固有のシナリオでの脅威ハンティングのためのカスタムモデル作成

Proficio のエンジニアリングチームは、PatternEx のデータ管理とデータレイクの統合機能、SOC ワークフロープロセスに適合する機能、AI モデルの処理に必要なリソース (ストレージとコンピューティング)、そして最後にサイバーキルチェーンにおける脅威のカバレッジとの AI モデルのパフォーマンスについても調査しました

“ PatternEx を使用して、完全に統合されたソリューションで MDR 機能に大きな価値を追加できました。私達は PatternEx という私達の将来の技術ニーズに合わせて一緒に進んでいけるパートナーを見つけました ”

Proficio の技術とセキュリティの SVP Jeremy Vance 氏。

PatternEx でもたらされるビジネスの拡大

セキュリティアナリストは、Proficio のクライアントに固有の脅威をより効率的かつ効果的に検出するために開発された 100 以上の構築済みモデルとカスタムモデルを開発できます。この機能は、Proficio の既存のクライアントの 25% 以上ですぐに採用され、今後グローバルクライアントの基盤を拡大していきます。

■ PatternEX 社について

<https://www.patternex.com/>

PatternEx は 2013 年に設立され、企業向けの「Analyst in the loop AI systems（アナリスト参加型 AI システム）」のリーダーであり、アナリストの生産性を向上させるために、人間とデータの相互作用の分野でいくつかの革新を実現してきました。MIT（マサチューセッツ工科大学）のコンピューター科学・人工知能研究所（CSAIL）を起源とする PatternEx は、人工知能の力と人間の直感を組み合わせて、セキュリティチームを拡大し、Virtual Analyst Platform を構築します。PatternEx はシリコンバレーに本社を置き、ニューヨーク、マドリッド、ニューデリーに拠点があります。

■ 株式会社 TwoFive 社について

<http://www.twofive25.com/>

株式会社 TwoFive は、大手 ISP、ASP、携帯事業者の電子メールシステムインフラで長年経験をつんだメールシステムの技術者集団により 2014 年に設立されました。日本の電子メール環境を向上させることを使命としてベンダーニュートラルな立場で最適な技術とサービスを組み合わせ、メールシステム的设计・構築、電子セキュリティなどについてコンサルティング、ならびに各種 Threat Intelligence を提供しています。

■ お問い合わせ

株式会社 TwoFive

Email : info@twofive25.com